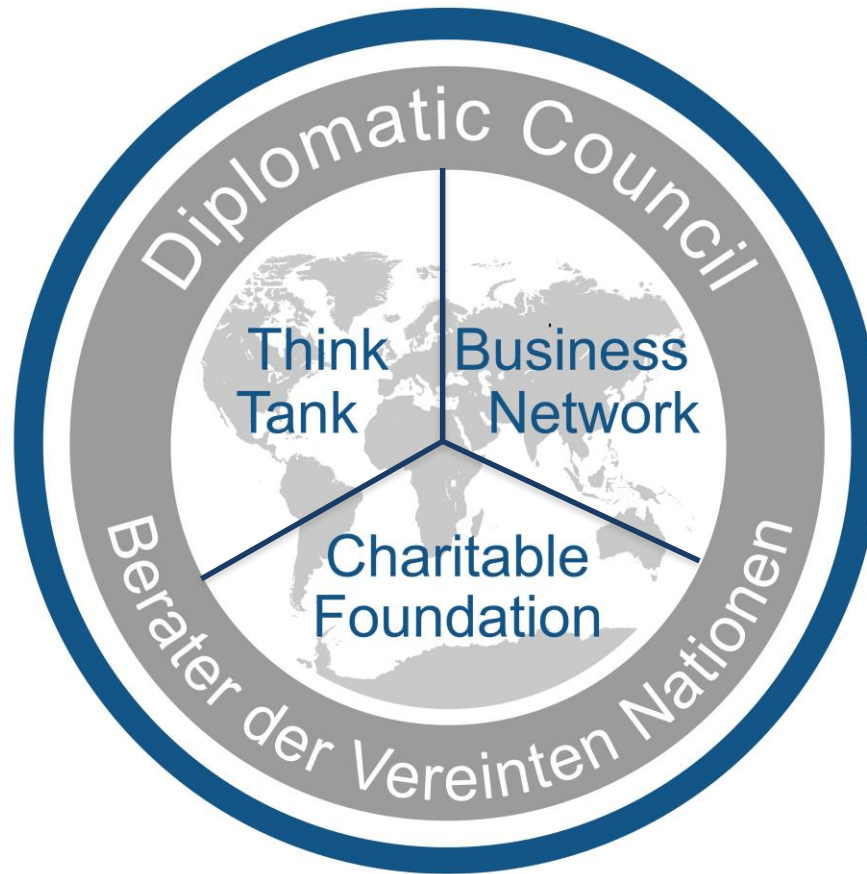


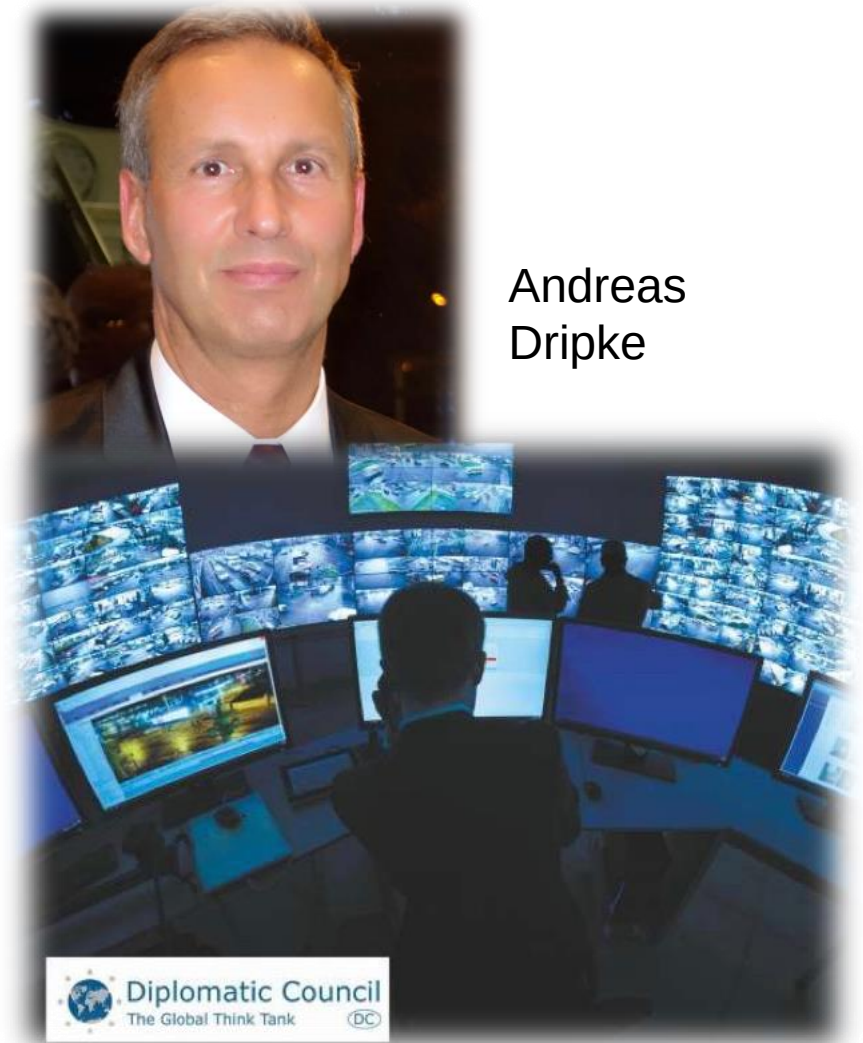


Andreas Dripke, Executive Chairman Diplomatic Council

Die dunkle Seite der Digitalisierung



Kapitel E-Spionage



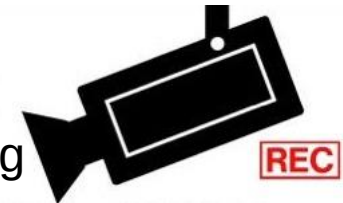
Staatssicherheit



Stasi 1.0:

Bis zu 2 Millionen von
9 Millionen DDR-Bürgern

ACHTUNG
Videoüberwachung



Stasi 2.0:

über 10 Milliarden Mikrofone,
Kameras und Sensoren bei
7 Milliarden Menschen weltweit

Der große Lauschangriff

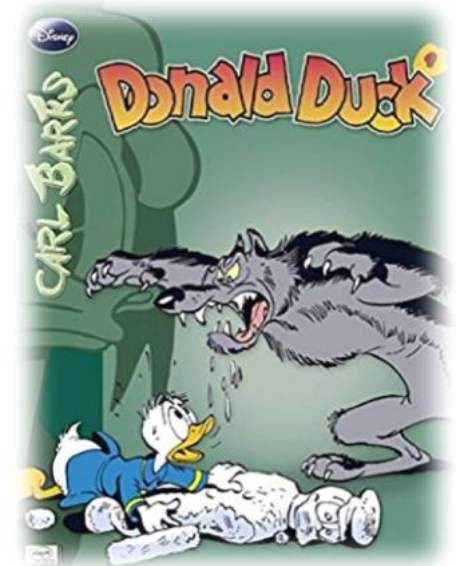
Donald Duck „Irrungen und
Wirrungen mit einem Werwolf“
(1968)

„Lauschangriff auf Bürger T“: Bundesamt für
Verfassungsschutz 1975. Manager Klaus Traube
wird in seiner eigenen Wohnung abgehört

Spiegel-Titel „Verfassungsschutz
bricht Verfassung“

16 Januar 1998: Bundestag beschließt
den „Großen Lauschangriff“

Erstmals räumt sich der Staat das Recht
ein, „seine“ Bürger in ihren eigenen vier
Wänden abzuhören.





Echolon = Wirtschaftsspionage im großen Stil

**Geheimes
Satelliten-
Spionage-
netzwerk**

**In Folge
des Zweiten
Weltkriegs**

**Arbeitete 50 Jahre im Verborgenen,
2000 setzte die EU einen Echolon—Ausschuss ein**



EU-Untersuchung 2001 beweist Existenz von Echolon

„Der Echelon-Ausschuss stellt fest, dass es keinen Zweifel mehr an der Existenz eines globalen Kommunikationsabhörsystems geben kann, das von den USA, Großbritannien, Australien, Neuseeland und Kanada betrieben wird.“

Bericht des Echolon-Ausschusses des Europäischen Parlaments

Echolon-Ziele:

- Nachrichtendienst
- Wirtschaftsspionage



Auch über die Zielsetzung des Systems, private und kommerzielle Kommunikation abzuhören, ist man sich einig.

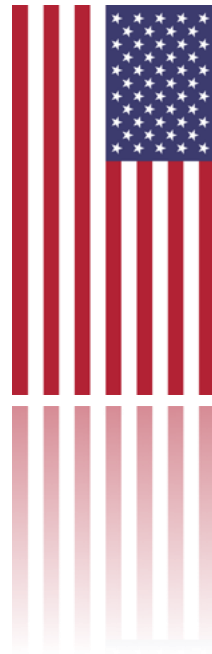
„Der Ausschuss kommt zu dem Schluss, dass bei einer Verwendung des Systems ausschließlich für nachrichtendienstliche Zwecke kein Verstoß gegen EU-Recht besteht; wenn das System jedoch dazu missbraucht wird, sich Wettbewerbs-vorteile zu verschaffen, steht dies in krassem Gegensatz zu der Verpflichtung der Mitgliedstaaten zu Loyalität mit dem Konzept des freien Wettbewerbs im Gemeinsamen Markt.“

20 Jahre nach dem “Großen Lauschangriff”



- EuGH genehmigt „Lauschangriff“ auf's Smartphone

- Zuvor nur bei schweren Vergehen, seit 02.10.2018 schon bei Verdacht auf leichte Straftaten
- Das Handy ist für die meisten Menschen das Konzentrat ihres Lebens.



Der globale Lauschangriff

- US Patriot Act 2001 gibt US-Behörden Zugang zu den Kundendaten aller US-Firmen
- Edward Snowden deckt 2013 auf: Die NSA hört die ganze Welt ab
- Cloud Act 2018: USA räumen sich selbst das Recht auf alle Daten überall auf der Welt ein

Cloud Act sei 2018

DSGVO ernst genommen bedeutet, dass Daten nicht in einem Rechenzentrum ausgelagert werden dürfen, das keinen Schutz vor ungeregeltem Zugriff der Geheimdienste bietet.

- Keine US-Unternehmen!
- Keine Unternehmen, in denen Server mit Chips arbeiten, die in China gefertigt wurden?



484612_Justitia_R_K_by_Thorben Wengert_pixelio.de

US Foreign Intelligence Surveillance Court (FISC)

- Geheimes US-Gericht zur Überwachung der Auslandsgeheimdienste, Urteil vom 29. August 2013 „Ein umfassender Lauschangriff ist konform mit der US-Verfassung selbst ohne richterlichen Beschluss.
- Damit sind alle gesetzeswidrigen Spionage-Aktivitäten von FBI, CIA und NSA legalisiert. Die Geheimdienste können alles tun - und sie tun es!

NSA Fusion Center in Utah



Datenzentrum für 7 Milliarden Menschen weltweit

1 Yotabyte = 10 000 000 000 000 000 000 000 000 Bytes

140 Gigabyte für jeden Menschen auf dieser Erde

Edward Snowden öffnete der Welt die Augen

1,9 Millionen geheime Dokumente
wurden 2013 öffentlich

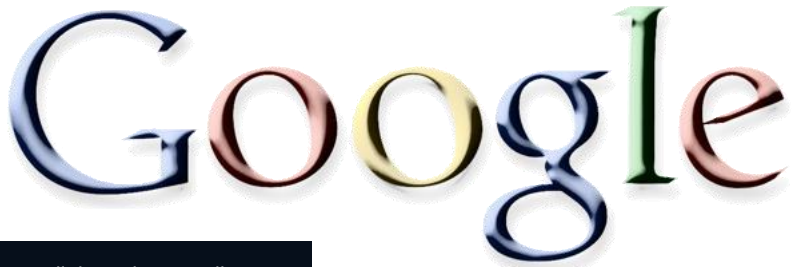
Ziele: UNO, EU, Bundesregierung...
Wirtschaft

Es wurde auch deutlich:
BND und NSA arbeiten Hand in Hand



E-Spionage als Geschäft: Google & Facebook

- Google - Datenmaximierung als Prinzip
- Spionage als Geschäftsmodell
- 80 Milliarden Dollar Werbeumsatz jährlich
- 86% aller Smartphones weltweit arbeiten mit Android
- Google sammelt binnen 10 Minuten mehr Daten als in der gesamten Geschichte der Menschheit vor 2000.



- 
- **Facebook - die größte Volkswirtschaft auf Erden**
 - **2 Milliarden „Bürger“ (China / Indien: jeweils ca. 1,3 Milliarden)**
 - **Facebook = Facebook + WhatsApp + Instagram**
 - **2,5 Milliarden Menschen nutzen täglich (!) eine der drei Apps**

SIEMENS



Unsere Kolleginnen und Kollegen

Erfahrungsberichte

Unser Controlling and Finance Assurance Programm hat schon viele erfolgreiche Führungspersönlichkeiten hervorgebracht. Hier erzählen sie, wie sie es nach oben geschafft haben.



Yan Ping (Alice) Li
Leiter of Mergers & Acquisitions für Asia und Australia, in China

Einfallstor Website und Social Media

- Facebook, Xing, LinkedIn - Ihre Beschäftigten outen sich
- Social Engineering: die unerkannte Gefahr
- 5 Minuten auf www.siemens.de fördert eine Schlüsselposition des Konzerns ans Licht.

Robin Sage - die Mata Hari des Cyberspace

25 Jahre alt, Absolventin der Technischen Hochschule in Massachusetts, Analystin für Cybersicherheit der US-Marine, zehn Jahre Berufserfahrung

Kurzes Leben: Dezember 2009 bis Januar 2010

Freundeskreis: 300 überwiegend hochrangige Personen aus US-Regierung, Militär und Wirtschaft

Schimäre von White Hat Hackern aus den USA



Die biometrische Vermessung

- Fingerabdrücke (Tatverdächtiger, US-Einreise, Smartphone)
- Automatische Gesichtserkennung (die unterschätzte Technik)
- Erkennung von Bewegungsabläufen („Testgelände“ Mannheimer Innenstadt)
- Gesten, Mimik, Gesundheit



Automatische Gesichtserkennung seit 2008 in Deutschland

- Bahnhof Berlin-Südkreuz: Test für die flächen-deckende Videoüberwachung in Deutschland
 - 80% Trefferquote, 0,3% Verwechslung
 - Bei 80 Millionen Bürgern sind das „nur“ 240.000 Verwechslungen
- Seit Anfang 2019: Automatisches Erkennen von Situationen (Verhaltens-Scanner)

Der Bio-Pass

- Seit 1.11.2010: Bio-Bild in jedem Ausweis/ Reisepass ab dem 6. Lebensjahr
- Ausweispflicht ab dem 16. Lebensjahr
- Die deutschen Behörden sammeln die biometrischen Daten von nahezu allen Deutschen
- RFID-Funkchip im Ausweis (2 m Reichweite)
- Der Fall Billie Hoffmann: Morphing der EU-Sicherheitspolitikerin Federica Mogherini
- Verfassungsbeschwerde seit 14. Juli 2014 anhängig



- Verdummung und Verharmlosung als Prinzip
- „Nicht im Chip abgelegt werden die eigenhändige Unterschrift, die Körpergröße und die Augenfarbe.“ (Bundesinnenministerium)
- Wer braucht das, wenn er Bio-Bild und Fingerabdrücke besitzt?
- Übrigens: Die Zerstörung des Chips ist eine Straftat

Biometrie – die sichere Täuschung



**PIN + Passwort =
alt und umständlich**

**Fingerabdruck und
Gesichtserkennung =
gefährlich!**

**PIN und Passwort können
wir ändern, unsere Finger,
unser Gesicht, unsere Art
uns zu bewegen, nicht**

Unsere Mimik verrät unsere Gefühle

iPhone X (seit 2017)

**True-Depth Kamera erfasst 30.000 Punkte im
Gesicht**

50 verschiedene Mikroausdrücke des Gesichts

Das heißt: Die Kamera erkennt unsere Gefühle!

**Hätten Sie es gewußt? Kameras können Lippen
lesen!**

ALLES SMART



Smart Watch:

Der Arzt am Handgelenk

Dauerkontrolle unserer Vitalwerte bis hin zum EKG

Smart Home: Alexa & Co

Wir holen uns die Spione freiwillig ins Haus

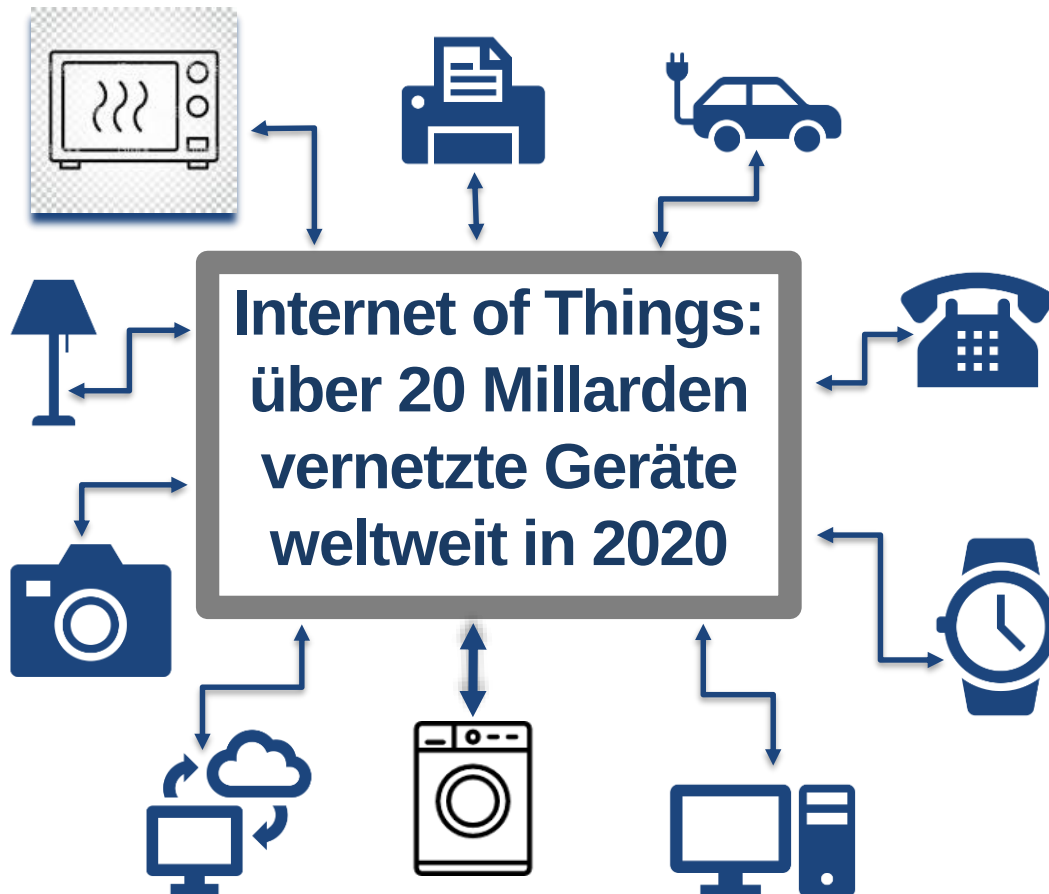


Smart City

Überwachung als Prinzip (UNO: 60% der Bevölkerung lebt 2030 in der Großstadt)



Smart Production and Smart Office



Industrie 4.0 wird Realität

88% der deutschen Firmen sind mit IoT-Projekten befasst (weltweit 85%)

Bosch, SAP u.v.a.m. wollen IoT-Schwergewichte werden

Künstliche Intelligenz – Paradies und Untergang



KI in Deutschland

- Geboren 1955 in den USA, am 18.7.2018 in Deutschland angekommen
- Bundesregierung: Deutschland soll „zum weltweit führenden Standort für KI werden“
- Der große Widerspruch: Big Data und Datenminimierung

Die wahren Täter

2009

- 3,4 Millionen Cyberangriffe

2013

- 3 Milliarden Nutzer-Account bei Yahoo geknackt

2015

- 59 Millionen Cyberangriffe

2017

- WannaCry - Warnung an die digitale Gesellschaft

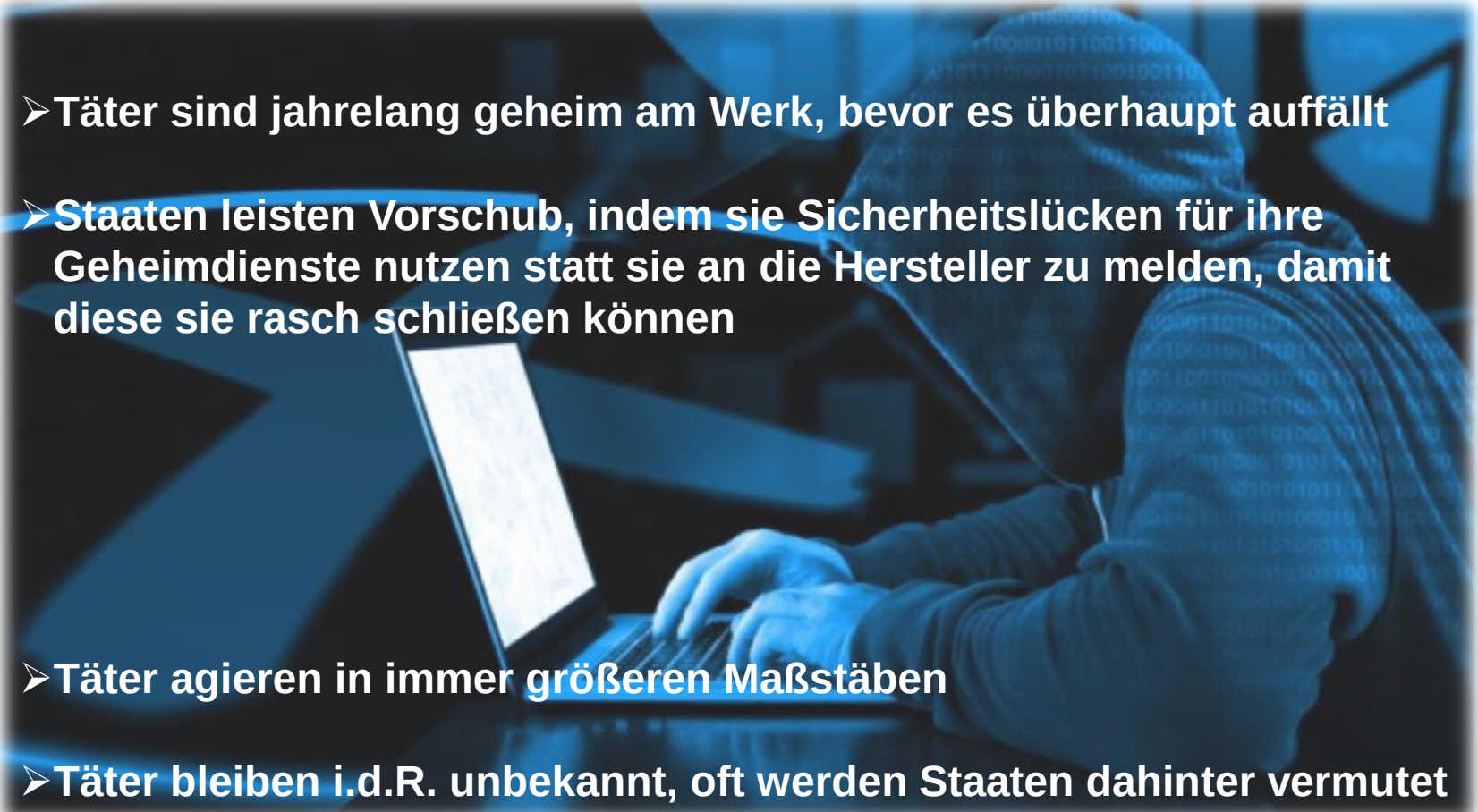
2018

- Adventskalender mit persönlichen Daten von 1000 Politiker und Promis

2019

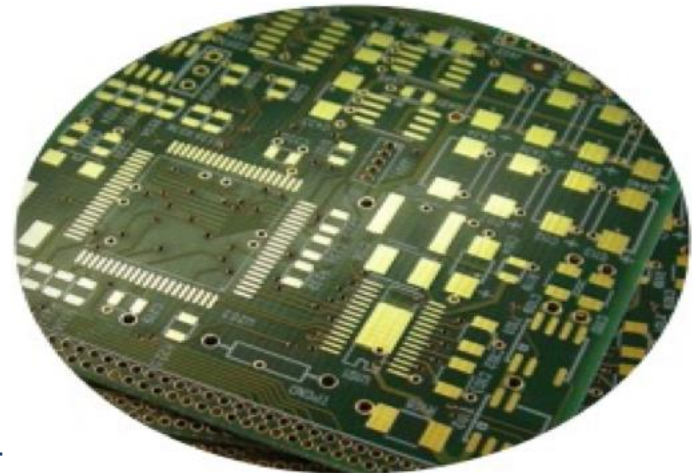
- 1,1 Milliarden E-Mail/Passwort-Kombinationen frei im Netz

Merkmale der Cyberkriminalität

- 
- **Täter sind jahrelang geheim am Werk, bevor es überhaupt auffällt**
 - **Staaten leisten Vorschub, indem sie Sicherheitslücken für ihre Geheimdienste nutzen statt sie an die Hersteller zu melden, damit diese sie rasch schließen können**
 - **Täter agieren in immer größeren Maßstäben**
 - **Täter bleiben i.d.R. unbekannt, oft werden Staaten dahinter vermutet**

Der Reiskorn-Hack 2018

- China hat Spionagechips auf die Computerplatinen von über 30 US-Firmen geschmuggelt
- Einsatz in den Cloud-Rechenzentren großer Digitalkonzerne wie u.a. Apple & Amazon
- 90% aller Computer und 75% aller Smartphones werden in China produziert
- Digitaler Generalangriff auf die westliche Welt



- Apple dementiert und verlagert die Produktion weg vom hauptbeschuldigten Platinenfertiger SuperMicro
- Handelskrieg USA - China = Cyberkrieg der Geheimdienste

Kampf der Kontinente



USA: Machtanspruch auf alle Daten weltweit



Europa: Schutz der Privatsphäre als Maxime



China, Russland & Co: Hack the World



Das blauäugige Deutschland wacht auf

- Von der Verteidigungs- zur Angriffsstrategie
- Schutz kritischer Infrastrukturen (Energie, Wasser, Ernährung...)
- Deutsche Hackerbehörde seit 2018 - ZITIS (Zentrale Stelle für Informationstechnik im Sicherheitsbereich). Cyberarmee der Angriffskrieger
- Bundesregierung beschuldigt erstmals Rußland öffentlich der Angriffe auf den Bundestag 2015, 2017 und 2018
- 2020: Lükex „Länderübergreifende Krisen-Exercise“

China: Der lange Marsch

China will 2049 die technologische Führungsrolle der Welt übernehmen.
100 Jahre Volksrepublik China.

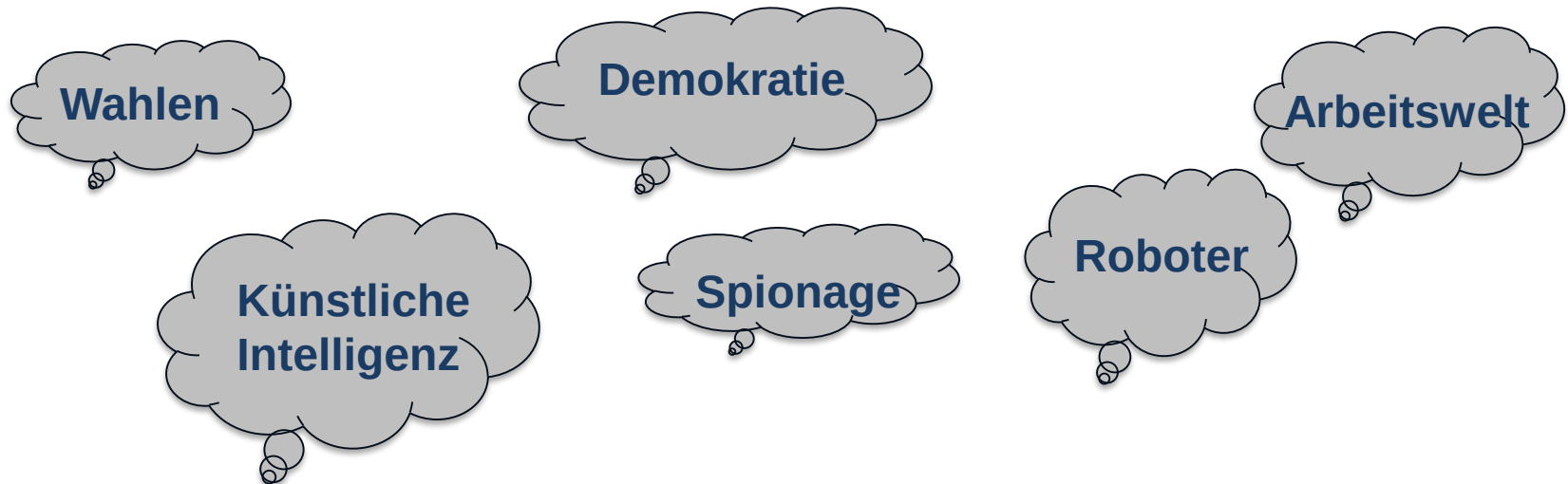
- USA:  am Black Friday über 1 Milliarde Dollar Umsatz an einem Tag
- China:  am Singles Day über 1 Milliarde Dollar Umsatz binnen 10 Minuten (22 Milliarden für den gesamten Tag)
- Deutschland: 160 Millionen Euro Umsatz am Tag im Online-Handel

China strebt die totale automatische Überwachung an

- ✓ 626 Millionen Kameras mit Gesichtserkennung ab 2020
- ✓ Social Scoring ab 2020 (gibt es seit 2018 auch bei Facebook)
- ✓ Smart Eye: Kameraüberwachung im Klassenzimmer mit Emotionserkennung
- ✓ Tauben als Augen und Ohren der Regierung

Gefahren der Digitalisierung

Die Verharmlosung der Digitalisierung gehört zu den schwersten Fehlern der modernen Gesellschaften.



= Politische, wirtschaftliche und gesellschaftliche Machtverschiebungen als Folge.

Zukunftsmensch

- ✓ **Chip-Implantate unmittelbar nach der Geburt**
- ✓ **Lückenlose Kamerakontrolle mit Identifizierung und Gefühlserkennung**
- ✓ **Künstliche Intelligenz regelt und steuert uns**

- 
- ✓ **Wir verhalten uns gesellschaftskonformer**
 - ✓ **Unser Leben wird angenehmer und bequemer**
 - ✓ **Wer in der Zukunft lebt, möchte nicht in unsere heutige Zeit zurück**